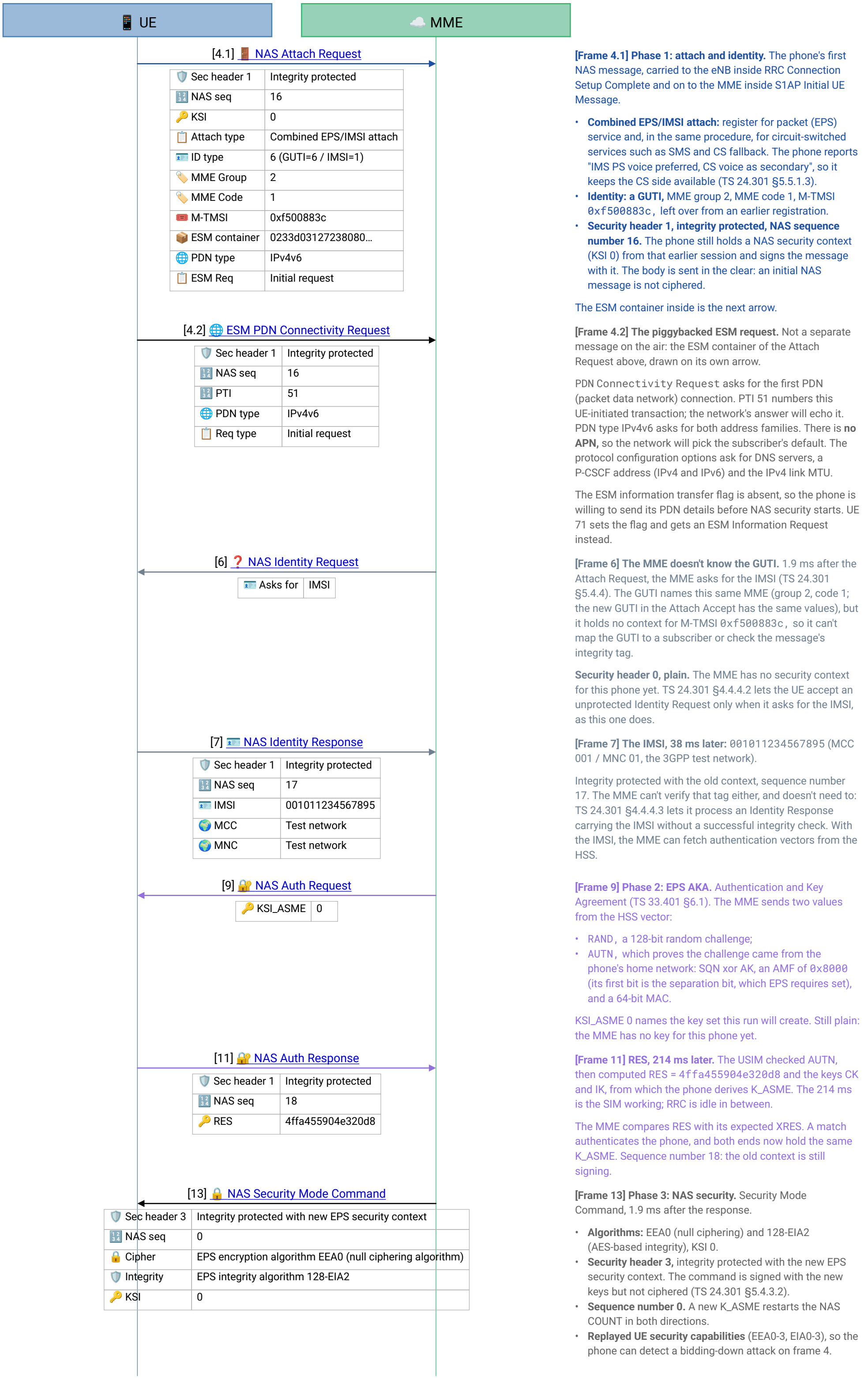
lte-nas-eps-attach-bearers.annotated



[Frame 4.1] Phase 1: attach and identity. The phone's first NAS message, carried to the eNB inside RRC Connection Setup Complete and on to the MME inside S1AP Initial UE Message.

- **Combined EPS/IMSI attach:** register for packet (EPS) service and, in the same procedure, for circuit-switched services such as SMS and CS fallback. The phone reports "IMS PS voice preferred, CS voice as secondary", so it keeps the CS side available (TS 24.301 §5.5.1.3).
- **Identity: a GUTI,** MME group 2, MME code 1, M-TMSI `0xf500883c`, left over from an earlier registration.
- **Security header 1, integrity protected, NAS sequence number 16.** The phone still holds a NAS security context (KSI 0) from that earlier session and signs the message with it. The body is sent in the clear: an initial NAS message is not ciphered.

The ESM container inside is the next arrow.

[Frame 4.2] The piggybacked ESM request. Not a separate message on the air: the ESM container of the Attach Request above, drawn on its own arrow.

PDN `Connectivity Request` asks for the first PDN (packet data network) connection. PTI 51 numbers this UE-initiated transaction; the network's answer will echo it. PDN type IPv4v6 asks for both address families. There is **no APN,** so the network will pick the subscriber's default. The protocol configuration options ask for DNS servers, a P-CSCF address (IPv4 and IPv6) and the IPv4 link MTU.

The ESM information transfer flag is absent, so the phone is willing to send its PDN details before NAS security starts. UE 71 sets the flag and gets an ESM Information Request instead.

[Frame 6] The MME doesn't know the GUTI. 1.9 ms after the Attach Request, the MME asks for the IMSI (TS 24.301 §5.4.4). The GUTI names this same MME (group 2, code 1; the new GUTI in the Attach Accept has the same values), but it holds no context for M-TMSI `0xf500883c`, so it can't map the GUTI to a subscriber or check the message's integrity tag.

Security header 0, plain. The MME has no security context for this phone yet. TS 24.301 §4.4.4.2 lets the UE accept an unprotected Identity Request only when it asks for the IMSI, as this one does.

[Frame 7] The IMSI, 38 ms later: `001011234567895` (MCC 001 / MNC 01, the 3GPP test network).

Integrity protected with the old context, sequence number 17. The MME can't verify that tag either, and doesn't need to: TS 24.301 §4.4.4.3 lets it process an Identity Response carrying the IMSI without a successful integrity check. With the IMSI, the MME can fetch authentication vectors from the HSS.

[Frame 9] Phase 2: EPS AKA. Authentication and Key Agreement (TS 33.401 §6.1). The MME sends two values from the HSS vector:

- `RAND`, a 128-bit random challenge;
- `AUTN`, which proves the challenge came from the phone's home network: SQN xor AK, an AMF of `0x8000` (its first bit is the separation bit, which EPS requires set), and a 64-bit MAC.

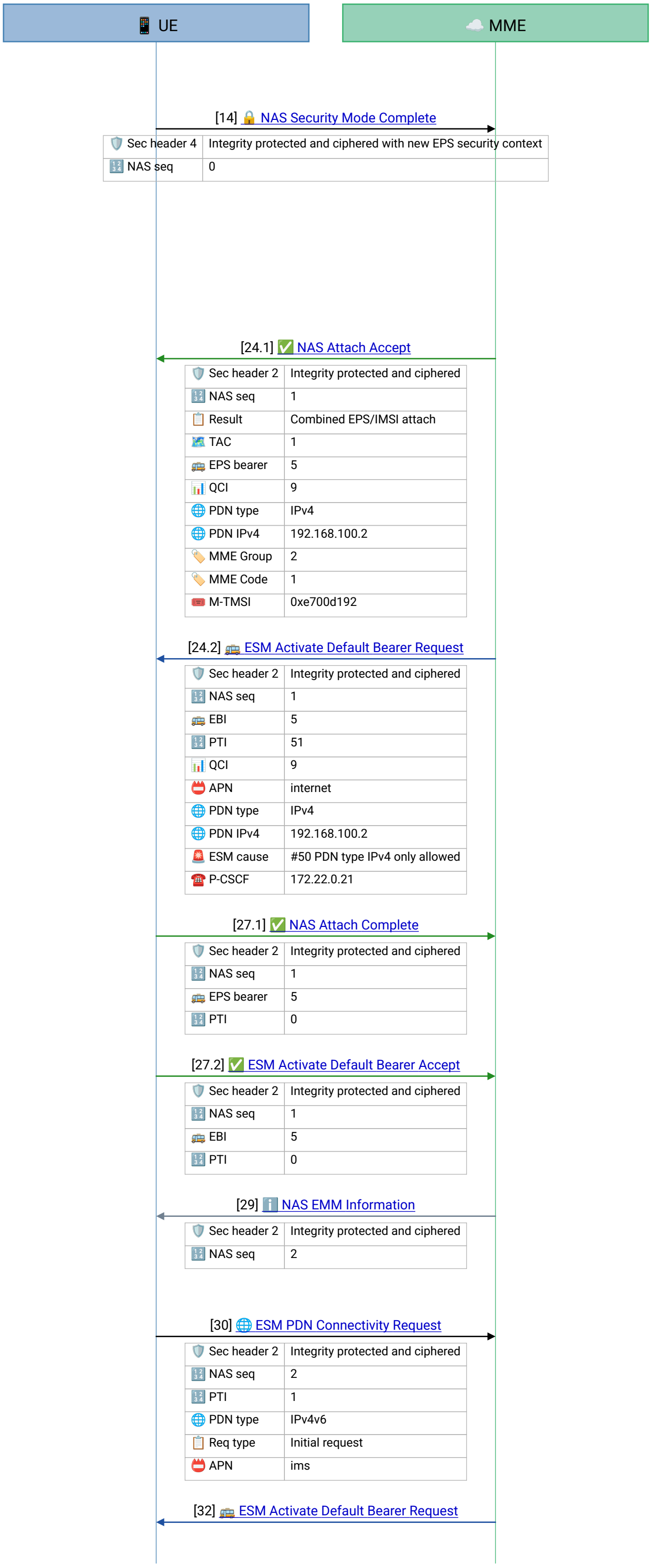
KSI_ASME 0 names the key set this run will create. Still plain: the MME has no key for this phone yet.

[Frame 11] RES, 214 ms later. The USIM checked AUTN, then computed RES = `4ffa455904e320d8` and the keys CK and IK, from which the phone derives K_ASME. The 214 ms is the SIM working; RRC is idle in between.

The MME compares RES with its expected XRES. A match authenticates the phone, and both ends now hold the same K_ASME. Sequence number 18: the old context is still signing.

[Frame 13] Phase 3: NAS security. Security Mode Command, 1.9 ms after the response.

- **Algorithms:** EEA0 (null ciphering) and 128-EIA2 (AES-based integrity), KSI 0.
- **Security header 3,** integrity protected with the new EPS security context. The command is signed with the new keys but not ciphered (TS 24.301 §5.4.3.2).
- **Sequence number 0.** A new K_ASME restarts the NAS COUNT in both directions.
- **Replayed UE security capabilities** (EEA0-3, EIA0-3), so the phone can detect a bidding-down attack on frame 4.



- **IMEISV request,** and **HashMME:** a hash of the Attach Request as the MME received it, sent because the MME couldn't check that message's integrity tag.

[Frame 14] Security Mode Complete. Security header 4: integrity protected and ciphered with the new context, sequence number 0. From here the phone uses only the new keys.

It returns the IMEISV the MME asked for. It does not include a replayed copy of the Attach Request, which it would if its own hash of frame 4 differed from HashMME (TS 24.301 §5.4.3.3). So frame 4 arrived unaltered.

Why "ciphered" still reads: with EEA0 the keystream is all zeros, so the ciphered bytes are the plaintext. They start `07 5e`: protocol discriminator 7 (EMM), message type `0x5e`, Security mode complete.

[Frame 24.1] Phase 4: Attach Accept. 94 ms after frame 14. The MME sent it to the eNB inside S1AP Initial Context Setup before the radio security started; the eNB held it through AS security and the capability exchange, then delivered it in RRC reconfiguration 1 with DRB 1.

Security header 2 (integrity protected and ciphered), sequence number 1.

- **Result:** combined EPS/IMSI attach accepted.
- **New GUTI:** M-TMSI `0xe700d192`, replacing the one the MME didn't know.
- **TAI list:** TAC 1. **T3412** (periodic tracking area update) and **T3423** both 54 min.
- **EPS network feature support:** IMS voice over PS session supported. This bit tells the phone it may use VoLTE here.

[Frame 24.2] The default bearer, inside the Attach Accept. `Activate Default EPS Bearer Context Request`, EBI 5, PTI 51 (frame 4's transaction):

- **APN `internet`,** the network's default, since frame 4 named none;
- **QCI 9,** best effort; APN-AMBR 1024 Mbps each way;
- **PDN type IPv4,** address `192.168.100.2`;
- **ESM cause #50, "PDN type IPv4 only allowed"** (TS 24.301 Annex B). The phone asked for IPv4v6; this cause says why it got IPv4 alone. It is an ESM cause in an accept, not a rejection.
- **PCO:** DNS 8.8.8.8 and 8.8.4.4, P-CSCF 172.22.0.21, IPv4 MTU 1300.

[Frame 27.1] Attach Complete, 26 ms later, the first message on SRB2. Sequence number 1 uplink: each direction keeps its own NAS COUNT, so this 1 and the Accept's 1 are unrelated.

UE 70 is now `EMM-REGISTERED`, 420 ms after its Attach Request.

[Frame 27.2] The default bearer accepted, in the Attach Complete's ESM container. EBI 5 names the bearer, and the PTI is 0.

EPS bearer 5 is active. On the radio it is DRB 1 on LCID 3.

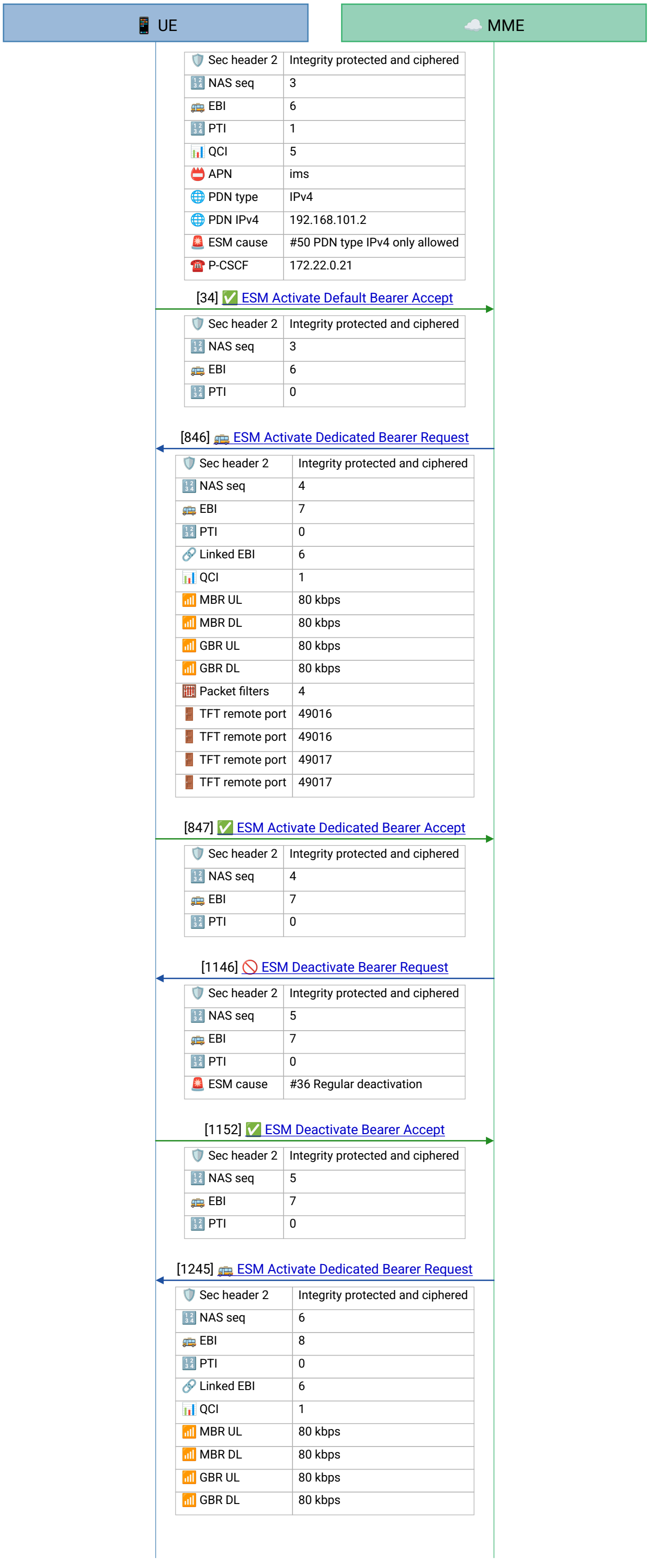
[Frame 29] EMM Information, 174 ms later. The network name, `Open5GS`, the open-source core this lab ran, and the local time zone, GMT+2, with universal time 08:28:28.

Optional (TS 24.301 §5.4.5). After the attach, it is the only downlink NAS message that doesn't ride inside an RRC reconfiguration. Sequence number 2.

[Frame 30] Phase 5: the IMS PDN. 6 ms later the phone asks for a second PDN connection, APN `ims`. VoLTE keeps SIP and voice on their own PDN, apart from internet traffic.

A standalone ESM message: the outer security header carries protocol discriminator 7 (EMM), because security protection is an EMM function, and the inner message carries 2 (ESM). New transaction, PTI 1. PDN type IPv4v6 again, and the PCO again asks for a P-CSCF. Uplink sequence number 2.

[Frame 32] The IMS default bearer, 8 ms later, inside RRC reconfiguration 2 with DRB 2.



EBI 6, PTI 1, APN `ims`, **QCI 5** (IMS signaling), address `192.168.101.2`, and ESM cause #50 again: IPv4 only. The PCO's P-CSCF, 172.22.0.21, is where the phone will send its SIP REGISTER. Downlink sequence number 3.

[Frame 34] Accepted, 32 ms later. EPS bearer 6 is active, on DRB 2. UE 70 now has its two PDN connections, `internet` on EBI 5 and `ims` on EBI 6, and NAS goes quiet for 23 s while the phone registers with IMS over EBI 6.

[Frame 846] Phase 6: six voice bearers. Call 1 added. UE 70 dialed in frame 821; UE 71's SIP 183 answered with media details, and the IMS core asked for a voice bearer. UE 71's came first, in frame 844.

`Activate Dedicated EPS Bearer Context Request:`

- **EBI 7, linked EBI 6:** it belongs to the IMS PDN and shares its IP address.
- **PTI 0:** network-initiated, no UE transaction to answer.
- **QCI 1,** conversational voice, guaranteed bit rate. **80 kbps** MBR and GBR each way. S1AP asked the eNB for 82,000 bit/s, but NAS encodes bit rates in steps, 8 kbps wide in this range, and 80 is the step below 82.
- **TFT,** 4 packet filters, all UDP to remote 172.22.0.16: port 49016 (RTP) downlink-only and uplink-only, then 49017 (RTCP) the same. 172.22.0.16:49016 is the media address the P-CSCF wrote into the 183.

[Frame 847] Accepted, 33 ms later. EBI 7, PTI 0, sequence number 4. EPS bearer 7 is active on DRB 3. From here the phone's uplink filter sends UDP to 172.22.0.16 port 49016 or 49017 down EPS bearer 7; all other traffic still matches nothing and stays on its PDN's default bearer.

[Frame 1146] Call 1 released, 6.4 s after the add. UE 71 sent BYE in frame 1143.

`Deactivate EPS Bearer Context Request`, EBI 7, PTI 0, **ESM cause #36, "regular deactivation"** (TS 24.301 Annex B). It rides the RRC reconfiguration that releases DRB 3.

[Frame 1152] Deactivation accepted, 40 ms later. EBI 7 is inactive. Here the RRC Reconfiguration Complete went up first, alone (frame 1148), and the NAS accept followed.

[Frame 1245] Call 2 added (UE 71 called). EBI 8, linked EBI 6, QCI 1, 80 kbps, the same four-filter TFT shape with remote ports 49028 and 49029. The MME didn't reuse EBI 7, though it has been free for 4.4 s: each call gets the next number.

📱 UE | ☁️ MME

🧱 Packet filters	4
🚪 TFT remote port	49028
🚪 TFT remote port	49028
🚪 TFT remote port	49029
🚪 TFT remote port	49029

[1248] ✅ ESM Activate Dedicated Bearer Accept →

[Frame 1248] Accepted, 26 ms later. EBI 8 active, on DRB 4.

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	6
🚌 EBI	8
🔢 PTI	0

[1503] 🚫 ESM Deactivate Bearer Request ←

[Frame 1503] Call 2 released, 6.5 s after the add. EBI 8, ESM cause #36.

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	7
🚌 EBI	8
🔢 PTI	0
🚨 ESM cause	#36 Regular deactivation

[1504] ✅ ESM Deactivate Bearer Accept →

[Frame 1504] Accepted, 32 ms later. EBI 8 inactive.

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	7
🚌 EBI	8
🔢 PTI	0

[1599] 🚌 ESM Activate Dedicated Bearer Request ←

[Frame 1599] Call 3 added (UE 71 called). EBI 9, remote ports 49054 and 49055. Everything else matches call 1.

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	8
🚌 EBI	9
🔢 PTI	0
🔗 Linked EBI	6
📊 QCI	1
📶 MBR UL	80 kbps
📶 MBR DL	80 kbps
📶 GBR UL	80 kbps
📶 GBR DL	80 kbps
🧱 Packet filters	4
🚪 TFT remote port	49054
🚪 TFT remote port	49054
🚪 TFT remote port	49055
🚪 TFT remote port	49055

[1603] ✅ ESM Activate Dedicated Bearer Accept →

[Frame 1603] Accepted, 37 ms later. EBI 9 active, on DRB 5.

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	8
🚌 EBI	9
🔢 PTI	0

[1926] 🚫 ESM Deactivate Bearer Request ←

[Frame 1926] Call 3 released, 6.7 s after the add. EBI 9, ESM cause #36.

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	9
🚌 EBI	9
🔢 PTI	0
🚨 ESM cause	#36 Regular deactivation

[1928] ✅ ESM Deactivate Bearer Accept →

[Frame 1928] Accepted, 33 ms later. EBI 9 inactive.

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	9
🚌 EBI	9
🔢 PTI	0

[2039] 🚌 ESM Activate Dedicated Bearer Request ←

[Frame 2039] Call 4 added (UE 70 called). EBI 10, remote ports 49086 and 49087.

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	10

📱 UE | ☁️ MME

🚌 EBI	10
🔢 PTI	0
🔗 Linked EBI	6
📊 QCI	1
📶 MBR UL	80 kbps
📶 MBR DL	80 kbps
📶 GBR UL	80 kbps
📶 GBR DL	80 kbps
🧱 Packet filters	4
🚪 TFT remote port	49086
🚪 TFT remote port	49086
🚪 TFT remote port	49087
🚪 TFT remote port	49087

[2042] ✅ ESM Activate Dedicated Bearer Accept →

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	10
🚌 EBI	10
🔢 PTI	0

[Frame 2042] Accepted, 38 ms later. EBI 10 active, on DRB 6.

[2316] 🚫 ESM Deactivate Bearer Request ←

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	11
🚌 EBI	10
🔢 PTI	0
🚨 ESM cause	#36 Regular deactivation

[Frame 2316] Call 4 released, 4.7 s after the add, the shortest call. EBI 10, ESM cause #36.

[2323] ✅ ESM Deactivate Bearer Accept →

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	11
🚌 EBI	10
🔢 PTI	0

[Frame 2323] Accepted, 39 ms later, again after a lone RRC Reconfiguration Complete (frame 2319). EBI 10 inactive.

[2447] 🚌 ESM Activate Dedicated Bearer Request ←

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	12
🚌 EBI	11
🔢 PTI	0
🔗 Linked EBI	6
📊 QCI	1
📶 MBR UL	80 kbps
📶 MBR DL	80 kbps
📶 GBR UL	80 kbps
📶 GBR DL	80 kbps
🧱 Packet filters	4
🚪 TFT remote port	49110
🚪 TFT remote port	49110
🚪 TFT remote port	49111
🚪 TFT remote port	49111

[Frame 2447] Call 5 added (UE 70 called). EBI 11, remote ports 49110 and 49111.

[2450] ✅ ESM Activate Dedicated Bearer Accept →

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	12
🚌 EBI	11
🔢 PTI	0

[Frame 2450] Accepted, 38 ms later. EBI 11 active, on DRB 7.

[2925] 🚫 ESM Deactivate Bearer Request ←

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	13
🚌 EBI	11
🔢 PTI	0
🚨 ESM cause	#36 Regular deactivation

[Frame 2925] Call 5 released, 11.7 s after the add, the longest call. EBI 11, ESM cause #36.

[2932] ✅ ESM Deactivate Bearer Accept →

[Frame 2932] Accepted, 29 ms later, after a lone Reconfiguration Complete (frame 2928). EBI 11 inactive.

📱 UE | ☁️ MME

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	13
🚌 EBI	11
🔢 PTI	0

[3032] 🚌 ESM Activate Dedicated Bearer Request

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	14
🚌 EBI	12
🔢 PTI	0
🔗 Linked EBI	6
📊 QCI	1
📶 MBR UL	80 kbps
📶 MBR DL	80 kbps
📶 GBR UL	80 kbps
📶 GBR DL	80 kbps
🧱 Packet filters	4
🧱 TFT remote port	49122
🧱 TFT remote port	49122
🧱 TFT remote port	49123
🧱 TFT remote port	49123

[Frame 3032] Call 6 added (UE 71 called). EBI 12, remote ports 49122 and 49123. On the radio this is DRB 8 on LCID 10, the last logical channel a DRB can use; see the RRC companion.

[3035] ✅ ESM Activate Dedicated Bearer Accept

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	14
🚌 EBI	12
🔢 PTI	0

[Frame 3035] Accepted, 36 ms later. EBI 12 active.

[3287] 🚫 ESM Deactivate Bearer Request

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	15
🚌 EBI	12
🔢 PTI	0
🚨 ESM cause	#36 Regular deactivation

[Frame 3287] Call 6 released, 6.1 s after the add. EBI 12, ESM cause #36: all six deactivations carry the same cause.

[3288] ✅ ESM Deactivate Bearer Accept

🛡️ Sec header 2	Integrity protected and ciphered
🔢 NAS seq	15
🚌 EBI	12
🔢 PTI	0

[Frame 3288] The last NAS message, 34 ms later. EBI 12 inactive, downlink and uplink sequence number both 15.

UE 70 ends as it was after frame 34: `EMM-REGISTERED`, EPS bearers 5 and 6 active. No detach, no tracking area update, no service request, and no EMM or ESM failure anywhere in the session. The capture ends 11 s later, as a seventh call begins; S1AP shows the MME asking for EBI 13.

Session Result: incomplete - mid-capture (duration: 1m 42.180s)