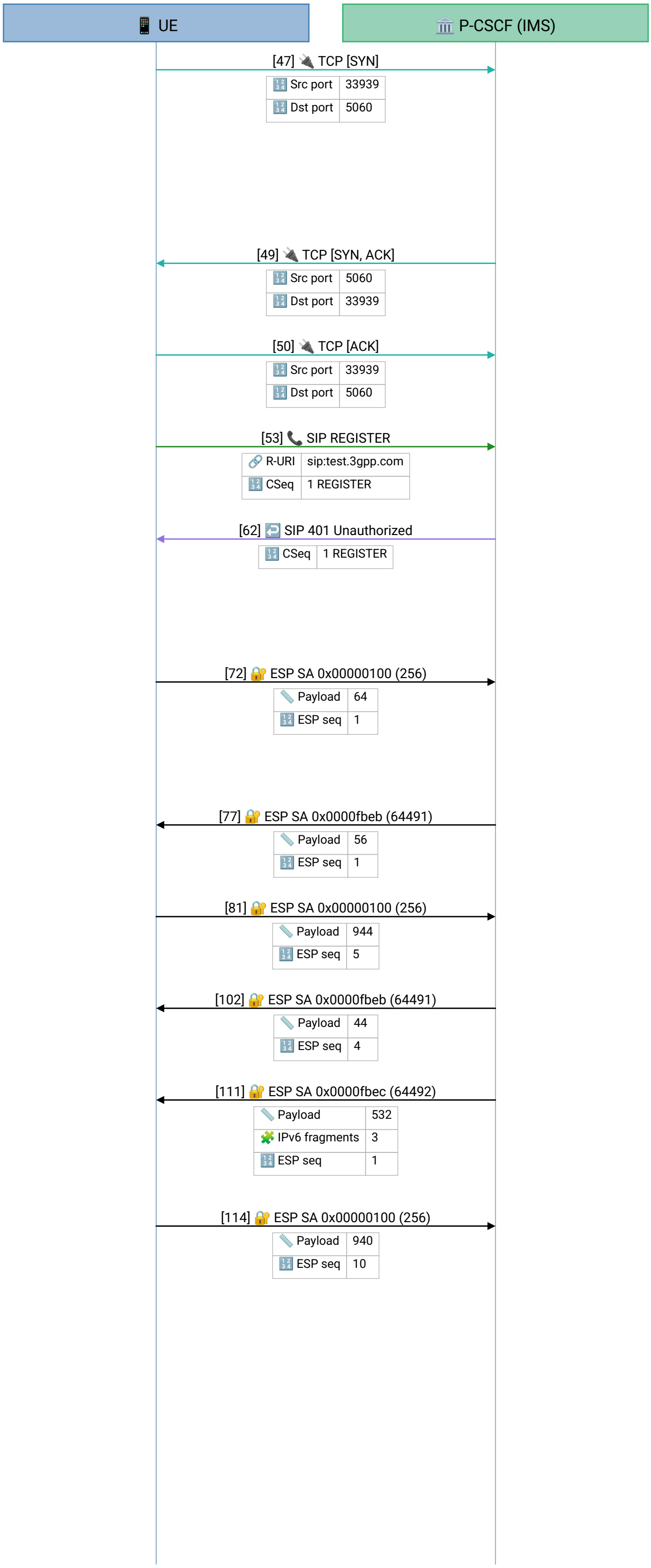

[Frame 47] The reveal begins. Everything on this diagram lived inside ciphered PDCP on DRB 1 until the published UE keys deciphered it — the radio-stack walkthrough saw only `UL SDAP -> QFI 2` here. With PDCP open, the SDAP payload turns out to be an ordinary IPv6 conversation, and it opens the way any TCP app does: a SYN from the UE (`port 33939`) to the P-CSCF on the SIP port `5060`. (The UE reached its global address `3000:0:0:2::2` moments earlier via IPv6 Router Solicitation / Advertisement — the SLAAC prefix `3000:0:0:2::` — which this diagram omits to keep the two lanes clean.)

[Frame 49] `SYN, ACK` from the P-CSCF — the standard TCP three-way handshake, now perfectly readable where a moment ago it was ciphertext.

[Frame 50] The UE's ACK completes the handshake. A TCP connection to the IMS edge on port `5060` is up; SIP can flow.

[Frame 53] SIP REGISTER. The UE's first IMS registration attempt, to `sip:test.3gpp.com`, `CSeq 1 REGISTER`. This is the IMS application talking — the reason a data bearer was built at all. It carries no credentials yet; in IMS-AKA the first REGISTER is expected to be challenged.

[Frame 62] 401 Unauthorized — the IMS-AKA challenge. The IMS core answers the bare REGISTER with a `401` carrying an authentication challenge (the `WWW-Authenticate` header, IMS-AKA per TS 33.203). This is the normal first leg of IMS registration, not a failure — the UE will now derive keys from the challenge and set up IPsec before re-registering. Note the ~1.2 s gap since the REGISTER: the challenge round-trips to the core.

[Frame 72] IPsec takes over — and SIP goes dark again. Right after the 401, IMS-AKA brings up IPsec ESP security associations between the UE and the P-CSCF, and all further SIP travels *inside* ESP. So having just deciphered the radio layer to read SIP, we watch the application deliberately re-encrypt itself at the IP layer. This first ESP packet is UE -> P-CSCF; the SPI `0x00000100` names the P-CSCF's inbound SA, and the per-SA sequence starts at `1`.

[Frame 77] The reverse-direction SA: P-CSCF -> UE, inbound SPI `0x0000fbeb`, sequence `1`. Two unidirectional SPIs, one each way, are one IPsec SA pair — ESP is always unidirectional, so a bidirectional exchange needs two.

[Frame 81] ESP on SPI `0x00000100` again, now at sequence `5`. The sequence climbs monotonically with no gaps or resets — a healthy SA carrying the protected SIP exchange, with no replay or rekey.

[Frame 102] The P-CSCF's SA (`0x0000fbeb`) at sequence `4`. The two directions advance independently, each with its own sequence space — exactly what you'd expect from a pair of one-way SAs.

[Frame 111] A **second** UE-inbound SA appears: SPI `0x0000fbec` (one more than `0x0000fbeb`), sequence `1`. IMS-AKA sets up more than one SA toward the UE (the protected client/server ports of TS 33.203), and this is the sibling coming into use. The packet is large enough to need IPv6 fragmentation — reassembled here from 3 fragments (payloads `1456 + 532`).

[Frame 114] Back on SPI `0x00000100`, sequence `10`: the UE -> P-CSCF SA has now carried ten protected packets. The IMS registration continues entirely inside IPsec from here, and the capture window closes — the point made, the once-opaque radio trace has given up its RRC, its SDAP QoS flow, and the IMS session riding on top.